UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,294	11/14/2003	Vincent J. Zimmer	42.P17570	1149

7590 05/29/2009

R. Alan Burnett
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
KIM, CHONG R	

ART UNIT	PAPER NUMBER
2624	

MAIL DATE	DELIVERY MODE
05/29/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,294	ZIMMER ET AL.	
	Examiner	Art Unit	
	CHARLES KIM	2624	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 21-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6 and 21-30* is/are rejected.

7)☒ Claim(s) *5 and 7-12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 3 and 6 are objected to due to typographical/grammatical errors.

Claim 3 recites "if is determined that" in line 2, which is grammatically incorrect. It appears Applicants intended the phrase to read "if it is determined that." Appropriate correction is required.

Claim 6 recites "versioning information,in an asset" in line 7. It appears Applicants intended the phrase to read "versioning information, in an asset." Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 25 and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Referring to claim 25, the phrase "to obtain the authenticated hash digest" in lines 5-6 lacks antecedent basis support. It appears that Applicants intended claim 25 to depend from claim 24, not claim 21. Appropriate correction is required.

Referring to claim 27, the phrase "each binary firmware image" in line 14 lacks antecedent basis support. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim(s) 21-26 is/are rejected under 35 U.S.C. 101 as encompassing non-statutory subject matter for at least the following reasons. MPEP 2106.01 states that "when functional descriptive material is recorded on some computer-readable medium, it becomes…statutory." Here, claims 21-26 recite functional descriptive material embodied on a "machine-readable medium." Because a "machine-readable medium" is broader in scope than MPEP 2106.01's requirement of a "computer-readable medium" and can include non-statutory subject matter such as a piece of paper, claims 21-26 are considered to be non-statutory.

In addition, claims 21-26, as properly read in light of the disclosure, is further non-statutory because the claims recite a "machine-readable medium," which is defined on paragraph 73 of the specification as encompassing statutory subject matter such as a "disk-based media," as well as ***non-statutory*** subject mater such as "carrier waves" and "signals." "A transitory, propagating signal … is not a 'process, machine, manufacture, or composition of matter.' Those four categories define the explicit scope and reach of subject matter patentable under 35 U.S.C. § 101; thus, such a signal cannot be patentable subject matter." *In re Nuijten,* 84 USPQ2d 1495, 1503 (Fed. Cir. 2007).

Because the full scope of the claims, as properly read in light of the disclosure, encompasses non-statutory subject matter (i.e., signal, carrier wave, etc.) the claims as a whole are non-statutory. The Examiner suggests amending "machine-readable medium" to "computer-

readable storage medium" to exclude the transitory/propagating subject matter described in the specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 6, 21-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Davis and Perry, U.S. Patent Application Publication No. 2005/0169496 ("Perry").

Referring to claim 1, Davis discloses a method, comprising:

building a steganographic extractor (cryptographic coprocessor) to extract hidden information contained in binary data [col. 3, l. 46-col. 4, l. 18. Note that hidden information is extracted in the authentication procedure.];

loading the steganographic extractor during a pre-boot phase of a computer system [col. 1, ll. 50-67 and col. 3, l. 46-col. 4, l. 18. Note that the authentication procedure is performed before the boot phase of a computer that has been rebooted.];

discovering, during the pre-boot phase, binary firmware data on which a steganographic operation has been performed to generate hidden information contained within each binary firmware data [col. 3, l. 46-col. 4, l. 18. Note that the authentication procedure discovers steganographically embedded information using public/private key cryptography.]; and

extracting, via the steganographic extractor during the pre-boot phase, the hidden information contained in each binary firmware data that is discovered [col. 3, l. 46-col. 4, l. 18].

Davis explains that the authentication procedure is performed on binary firmware data, as noted above, but does not explicitly disclose that the authentication procedure is performed on *image* data. However, this feature was well known in the art. For example, Perry discloses a similar authentication method that authenticates non-image firmware data as well as image data [pars. 36 and 40].

Davis and Perry are combinable at least because they are both concerned with authenticating firmware. Using Perry's image data in place of Davis's non-image data represents a simple substitution of one well known type of data for another equally well known type of data. The ordinary skilled and creative artisan, with full recourse to common sense, at the time of the invention would have found it obvious to modify Davis's authentication procedure so that it is performed on image data, as taught by Perry. The reason for doing so would have been to achieve the known and predictable result of determining whether an image is authentic. Moreover, adding Perry's teaching to Davis's method would have enhanced the flexibility of the authentication process by providing the capability of authenticating a variety of different types of data, such as non-image data as well as image data.

Referring to claim 2, Davis further discloses obtaining a digital signature contained in the hidden information that is extracted from one of the binary fire, ware images; comparing the digital signature with a known authentic digital signature to determine an authenticity of that binary firmware image [col. 3, l. 60-col. 4, l. 18].

Referring to claim 3, Davis further discloses loading the binary firmware image if it is determined that the digital signature that is extracted matches the known authentic digital signature [col. 3, l. 60-col. 4, l. 18].

Referring to claim 4, Perry further discloses providing a notification message to a user indicating that data could not be authenticated if it is found that a digital signature does not match a known authentic signature [pars. 37-38].

Referring to claim 6, Davis further discloses that the hidden information that is extracted contains at least one of manufacturer and versioning information, wherein the method further comprising: obtaining said at least one of manufacturer and versioning information from the hidden information; and storing said at least one of manufacturer and versioning information in an asset management log [col. 4, ll. 19-46].

Referring to claim 21, see the rejection of at least claim 1 above. Davis further discloses a machine-readable medium to provide instructions for performing the method recited in claim 1 [fig. 1].

Referring to claim 22, see the rejection of at least claim 1 above.

Referring to claim 23, see the rejection of at least claim 2 above.

Referring to claim 24, Davis further discloses performing the operations of: determining op code sequences that are identifiable to the steganographic extractor as representing steganographic data [col. 3, l. 61-col. 4, l. 19].

Davis does not explicitly disclose performing a hash operation on the steganographically embedded data. However, this feature was well known in the art. For example, Perry discloses performing a hash on a portion of an image that represent steganographic data to obtain an image

hash digest; extracting an authenticated hash digest and comparing the image hash digest to the authenticated hash digest to determine an authenticity of the image data [par. 97].

As noted above, Davis and Perry are combinable because they are both concerned with authenticating firmware. Davis explains that a variety of authentication techniques may be used to authentic the firmware data [col. 4, l. 4]. Perry provides one type of well known authentication technique that performs a hashing operation on image data. One of ordinary skill and creativity, starting with Davis, would have looked to Perry to incorporate the hashing operations, in order to achieve the known and predictable result of authenticating the firmware data in a secure and accurate manner.

Referring to claim 25, Perry further discloses retrieving a decryption key and decrypting the hidden information that is extracted with the decryption key to obtain the authenticated hash digest [pars. 29-30].

Referring to claim 26, Davis further discloses retrieving asset management information from the hidden information that is extracted and storing the asset management information that is retrieved [col. 4, ll. 19-46].

Referring to claim 27, see the rejection of at least claim 1 above. Davis further discloses a processor, a memory coupled to the processor, and a flash device coupled to the processor for performing the method recited in claim 1 [see fig. 1].

Referring to claim 28, see the rejection of at least claim 1 above.

Referring to claim 29, see the rejection of at least claim 24 above.

Referring to claim 30, Davis further discloses retrieving a public key stored in the computer system corresponding to the private key; and employing the public key to decrypt the

hidden information that is extracted from one of the binary firmware drivers [col. 3, l. 61-col. 4, l. 46].

Allowable Subject Matter

5. Claims 5, 7-12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles Kim whose telephone number is 571-272-7421. The examiner can normally be reached on Mon thru Thurs 8:30am to 6pm and alternating Fri 9:30am to 6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Samir Ahmed can be reached on 571-272-7413. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/CHARLES KIM/
Primary Patent Examiner
Art Unit 2624
charles.kim@uspto.gov

May 22, 2009